3/9/2000
~~Exact~~ Search
STN/APS

08989261

```
$%^STN;HighlightOn=  ***;HighlightOff=***  ;
=> d hist


     (FILE 'HOME' ENTERED AT 14:21:34 ON 29 FEB 2000)

     FILE 'USPATFULL' ENTERED AT 14:21:40 ON 29 FEB 2000
L1             0 S DIFFERENT (2A) ALGORITHM# (2A) ENCRYPTION (3A) BLOCK
#
L2             0 S DIFFERENT (2A) ALGORITHM# (2A) ENCRYPTION (3A) SEGME
NT#
L3            79 S DIFFERENT (2A) ALGORITHM# (2A) ENCRYPTION
L4            12 S L3 (P) (SEGMENT# OR BLOCK#)
L5             2 S ENCRYPTION OBJECT
L6             0 S 5577125.PN.
L7             0 S 5577125/PN
L8             0 S 5577125
L9             1 S L5 AND (DOUBLE CLICKING)
L10            0 S L9 AND OOP
L11            0 S L9 AND (OBJECT ORIENTED)
L12         3681 S OBJECT ORIENTED
L13           15 S L12 AND ENCRYPTION (2A) OBJECT

:1


L19  ANSWER 1 OF 1  USPATFULL
AB     An access control processor for a conditional access system in
which
       ***encrypted***   information   ***segments***   provided by a
plurality
       of information service providers are encrypted for transmission
 in
       accordance with different conditional access processes respecti
vely
       utilizing   ***different***     ***algorithms***   for encrypti
ng the
       information segments. The processor includes a decryptor in an
       information receiver by decrypting encrypted information segmet
s
       received by the information receiver by processing the received
       ***encrypted***   information   ***segments***   with a session
 key used
       for encrypting the information segments in accordance with an a
lgorithm
       utilized in one of said.  .  .  access processes; and a conditi
onal
       access controller in the information receiver for selectively e
```

nabling
the decryptor to decrypt received information ***segments***

encrypted in accordance with any of said different cond
itional
access processes by providing to the decryptor cryptographic in
formation
for defining the. . . utilized in said one of said different
conditional access processes for use by the decryptor to decryp
t the
received information ***segment*** ***encrypted*** in a
ccordance
with said algorithm. Algorithm-defining cryptographic informati
on is
downloaded from an information stream received by the informati
on
receiver. Transmission. . .

SUMM In the prior art, ***encrypted*** information ***segments
***
respectively provided by a plurality of different conditional a
ccess
information service providers are respectively encrypted for
transmission in accordance with different conditional access pr
ocesses,
which may respectively utilize ***different*** ***algorit
hms***
for encrypting the information segments; and the differently
encrypted information ***segments*** are respective
ly
decrypted by differently configured information receivers respe
ctively
containing access control processors adapted for enabling decry
ption of
only ***encrypted*** information ***segments***
encrypted in accordance with one of the different condi
tional
access processes. An encryption algorithm is a process by which
a given.
. .

SUMM . . . Klein S. Gilhousen, Jerrold A. Heller, Michael V. Hard
ing and
Robert D. Blakeney. In such conditional access system, an infor
mation
segment is ***encrypted*** for transmission by scra
mbling
the information segment with a keystream that is produced by pr
ocessing
a secure session key in. . . algorithm. In an information re

ceiver of
such a conditional access system, the encrypted information sig
nal is
decrypted by descrambling the ***encrypted*** information
segment with a keystream that is produced by processing
the
secure session key in accordance with the predetermined encrypt
ion
algorithm. The. . . is processed to produce the keystream th
at is
used to scramble an information segment for a given transmissio
n of the
encrypted information ***segment*** . Typically the
session
key is processed with another key and/or a data signal to produ
ce the
keystream. In the two. . .

SUMM The prior art has suggested a conditional access system that wo
uld
enable ***encrypted*** information ***segments*** respe
ctively
encrypted for transmission in accordance with different
conditional access processes to be descrambled through use of a
standard
information receiver having. . . the different conditional a
ccess
information service providers for enabling a common descrambler
in the
information receiver to descramble received information ***se
gments***
encrypted in accordance with any of the different condi
tional
access processes. In such a system the use of a common descramb
ler to
decrypt ***encrypted*** information ***segments*** prov
ided by
any of a plurality of different information service providers t
hat
respectively ***encrypt*** information ***segments*** f
or
transmission in accordance with any of a plurality of different
conditional access processes respectively utilizing ***differ
ent***
algorithms for encrypting the information segments woul
d make it
necessary that each of the detachable conditional access module
s
respectively provided by. . .

SUMM The present invention provides an access control processor for a conditional access system in which ***encrypted*** information ***segments*** provided by a plurality of information service providers are encrypted for transmission in accordance with different conditional access processes respectively utilizing ***different*** ***algorithms*** for encrypting the information segments, the processor comprising a decryptor in an information receiver for decrypting ***encrypted*** information ***segments*** received by the information receiver by processing the received ***encrypted*** information ***segments*** with a session key used for encrypting the information segments in accordance with an algorithm utilized in one of said. . . access processes; and a conditional access controller in the information receiver for selectively enabling the decryptor to decrypt received information ***segments*** ***encrypted*** in accordance with any of said different conditional access processes by providing to the decryptor cryptographic information for defining the. . . utilized in said one of said different conditional access processes for use by the decryptor to decrypt the received information ***segment*** ***encrypted*** in accordance with said algorithm.

The cryptographic information for defining the encryption algorithm may define various bit selection and/or processing. . .

SUMM . . . be contained in a detachable conditional access module that would be interfaced with the information receiver for enabling decryption of ***encrypted*** information ***segments*** provided by such service provider, thereby reducing the cost of the detachable conditional access modules, which are replaced from time. .

SUMM . . . present invention also provides a conditional access s

ystem
including the above-described access control processor in combi
nation
with encryption means for ***encrypting*** information
segments for transmission in accordance with different
conditional access processes respectively utilizing ***differ
ent***
algorithms for encrypting the information segments.
SUMM - In another aspect, the present invention provides an access con
trol
processor for a conditional access system in which an ***encr
ypted***
information ***segment*** provided by an information servic
e
provider is encrypted for transmission in accordance with a con
ditional
access process utilizing an algorithm for encrypting the inform
ation
segment, the processor comprising a decryptor in an information
receiver
for decrypting ***encrypted*** information ***segments***

received by the information receiver by processing the received
encrypted information ***segments*** with a session
key used
for encrypting the information segments in accordance with an a
lgorithm
utilized in said conditional access process; and a conditional
access
controller in the information receiver for enabling the decrypt
or to
decrypt received information ***segments*** ***encrypted*
** in
accordance with said conditional access process by providing to
the
decryptor cryptographic information for defining the algorithm
utilized
in said conditional access process for use by the decryptor to
decrypt
the received information ***segments*** ***encrypted***
in
accordance with said algorithm, wherein the conditional access
controller includes means for detecting within an information s
tream
received by the information receiver cryptographic information
for
defining the algorithm used for ***encrypting*** informatio
n

segments in accordance with said conditional access process; and

means for downloading the detected cryptographic information from said information stream.

SUMM In a further aspect, the present invention provides an access control processor for a conditional access system in which an ***encrypted*** information ***segment*** provided by an information service provider is encrypted for transmission in accordance with a given conditional access process, the processor comprising a decryptor in an information receiver for decrypting ***encrypted*** information ***segments*** received by the information receiver; and a conditional access controller in the information receiver for enabling the decryptor to decrypt received information ***segments*** ***encrypted*** in accordance with the given conditional access process; wherein the conditional access controller includes means for requesting transmission to the. . .

DETD . . . information service provider A for transmission in accordance with a first conditional access processes utilizing a first algorithm A for ***encrypting*** information ***segments*** 14a; and a second information server 10b encrypts clear information segments 14b provided by a second information service provider B. . .

DETD . . . a session key K in accordance with the first algorithm A utilized in the first conditional access process to provide ***encrypted*** information ***segments*** 23. The session key K is included in cryptographic information 24 that is processed by the entitlement message generator 20 with entitlement information 25 to provide entitlement messages 26. The encoder 22 combines the ***encrypted*** information ***segments*** 23 and entitle

ment
messages 26 to provide a combined signal 27 for transmission. E
xamples
of entitlement information are described in. . .
DETD The demultiplexer 33 demultiplexes a received combined signal 3
8
containing ***encrypted*** information ***segments*** a
nd
entitlement messages and provides the received ***encrypted**
*
information ***segments*** 23 to the decryptor 31 and the r
eceived
entitlement messages 26 to the conditional access controller 32
.
DETD . . . processes the entitlement messages 26 to determine whe
ther the
decryptor 31 in the information receiver 12 is authorized to de
crypt
encrypted information ***segments*** 23 identified
by the
service request signal 40. Upon determining that the decryptor
31 and
thereby the information receiver 12. . . 32 provides appropr
iate
cryptographic information 42 to the decryptor 31 to thereby ena
ble the
decryptor 31 to decrypt the received ***encrypted*** inform
ation
segments 23. The cryptographic information 42 includes
the
session key K and cryptographic data for defining the algorithm
A or B
utilized in the conditional access process used to produce the
encrypted information ***segments*** 23 identified
by the
service request signal 40.
DETD The decryptor 31 then decrypts the received ***encrypted***
information ***segments*** 23 by processing the received
encrypted information ***segments*** 23 with the se
ssion key
K used for encrypting the information segments in accordance wi
th the
algorithm A or B utilized in the conditional access process use
d to
produce the ***encrypted*** information ***segments***
23, to
thereby reproduce the clear information segments 14, which are
provided

to the information processor 35.

DETD The decryptor 51 receives a combined signal 58 containing ***encrypted*** information ***segments*** and entitlement messages.

DETD . . . decryptor 51 is enabled for decryption, the combined signal 59 provided from the decryptor 51 to the demultiplexer 53 includes ***encrypted*** information ***segments*** .

DETD . . . processes the entitlement messages 60 to determine whether the decryptor 51 in the information receiver 49 is authorized to decrypt ***encrypted*** information ***segments*** identified by the service request signal 62. Upon determining that the decryptor 51 and thereby the information receiver 49 is. . . 52 provides appropriate cryptographic information 64 to the decryptor 51 to thereby enable the decryptor 51 to decrypt the received ***encrypted*** information ***segments*** included in the received combined signal 58. The cryptographic information 64 includes the session key K and cryptographic data for defining the algorithm A or B utilized in the conditional access process used to produce the ***encrypted*** information ***segments*** identified by the service request signal 62. Since the combined signals 27a provided by the information server 10a of information service provider A may incorporate the ***encrypted*** information ***segments*** into the combined signal 27a in a different format than the format used for such purpose by the information server. . . 51 by the conditional access controller 52 further includes format data that enables the decryptor 51 to decrypt only the ***encrypted*** information ***segments*** included in the combined signal 58.

DETD . . . decryption, the combined signal 59 provided from the decryptor 51 to the demultiplexer 53 includes clear information segments

rather
than ***encrypted*** information ***segments*** .
DETD The decryptor 51 decrypts the received ***encrypted*** info
rmation
segments in the combined signal 58 by processing the re
ceived
encrypted information ***segments*** with the sessi
on key K
used for encrypting the information segments in accordance with
the
algorithm A or B utilized in the conditional access process use
d to
produce the ***encrypted*** information ***segments*** ,
to
thereby reproduce the clear information segments 14, which are
provided
by the multiplexer 53 to the information processor 55.
DETD . . . 82 stored in the memory 74 to determine whether the de
cryptor
31 in the information receiver is authorized to decrypt
encrypted information ***segments*** identified by
the
service request signal 40. Upon determining that the decryptor
31 and
thereby the information receiver is so. . .
DETD . . . to thereby provide to the decryptor 31 the cryptograph
ic
information 42 that enables the decryptor 31 to decrypt the rec
eived
encrypted information ***segments*** 23 identified
by the
service request signal 40. As indicated above, the cryptographi
c
information 42 includes the session key K. . . and cryptogra
phic
information for defining the algorithm A or B utilized in the
conditional access process used to produce the ***encrypted**
*
information ***segments*** identified by the service reques
t signal
40.
DETD . . . identified in the service request signal 40. In one em
bodiment,
the memory 74 stores the cryptographic information for defining
the
different ***algorithms*** A and B respectively use
d in the
different conditional access processes. In another embodiment t

he
cryptographic information for defining each. . . 75 respecti
vely
provided by the different conditional access information servic
e
providers and respectively storing the cryptographic informatio
n for
defining the ***different*** ***algorithms*** A, B util
ized for
decrypting the received ***encrypted*** information ***se
gments***
23 in accordance with the different conditional access processe
s A and
B.
DETD . . . of the service providers; and selects for decryption i
n
accordance with a predetermined priority based upon such status
determinations the ***encrypted*** information ***segment
***
provided by one of the service providers. Examples of different
statuses
include, in order of priority: "blacked-out", "locked-out",
"authorized", "available. . .
DETD . . . in the information receiver to determine that the decr
yptor 31
in the information receiver is authorized to decrypt the select
ed
encrypted information ***segment*** . If the cryptog
raphic
information generator 72 is of the type described in the aforem
entioned
U.S. Pat. No. 4,712,238, at least. . .
DETD . . . algorithm that is used in the conditional access proce
ss
utilized by the information server 10a, 10b that encrypts the s
elected
encrypted information ***segment*** and cryptograph
ic data
for use in generating a session key for use by the decryptor 32
for
decrypting information ***segments*** ***encrypted*** i
n
accordance with the given conditional access process, including
data for
defining an algorithm for generating the session key and. . .

DETD . . . receiver 12, 49 includes all of the possible status me
ssages 94

in addition to the entitlement messages 26 and the ***encrypted*** information ***segments*** 23. In this embodiment, the conditional access controller 32, 52 includes a control processor 95, an authorization processor 96, a. . .

DETD . . . to thereby provide to the decryptor 31 the cryptographic information 42 that enables the decryptor 31 to decrypt the received ***encrypted*** information ***segments*** 23 identified by the service request signal 40.

DETD . . . by the information provider. Hence each conditional access service provider can customize its own conditional access algorithms, including the information ***segment*** ***encryption*** algorithm. Accordingly the required integrated circuit sets in a present day proprietary network interface module are replaced by the access. .

.

CLM What is claimed is:

. . . by a plurality of information service providers are encrypted for transmission in accordance with different conditional access processes respectively utilizing ***different*** ***algorithms*** for encrypting the information segments, the processor comprising a decryptor in an information receiver for decrypting ***encrypted*** information ***segments*** received by the information receiver by processing the received ***encrypted*** information ***segments*** with a session key used for encrypting the information segments in accordance with an algorithm utilized in one of said. . . access processes; and a conditional access controller in the information receiver for selectively enabling the decryptor to decrypt received information ***segments*** ***encrypted*** in accordance with

any of said different conditional access processes by providing to the decryptor cryptographic information for defining the. . . utilized in said one of said different conditional access processes for use by the decryptor to decrypt the received information ***segment*** ***encrypted*** in accordance with said algorithm.

. . . means for detecting within an information stream received by the information receiver cryptographic information for defining the algorithm used for ***encrypting*** information ***segments*** in accordance with said one of said different conditional access processes; and means for downloading the detected cryptographic information from. . .

. . . claim 1, wherein the conditional access controller includes a memory in the information receiver storing cryptographic information for defining said ***different*** ***algorithms*** respectively utilized in said different conditional access processes.

. . . service providers; and means for selecting for decryption in accordance with a predetermined priority based upon said status determinations the ***encrypted*** information ***segment*** provided by one of said service providers.

. . . algorithm provided by the conditional access controller to the decryptor is provided in accordance with said selection of the selected ***encrypted*** information ***segment*** provided by said one service provider.

. . . combination with a demultiplexer in the information receiver, wherein the demultiplexer is adapted for demultiplexing a received combined signal containing ***encrypted*** information ***segments*** and entitlement messages; wherein the decryptor is coupled to the demultiplexer for receiving the demultiplexed ***encrypted***

information ***segments*** for said decryption, and wherein the conditional access controller is coupled to the demultiplexer for receiving the demultiplexed entitlement messages. . . . . according to claim 1 in combination with a demultiplexer in the information receiver, wherein the decryptor is adapted for decrypting ***encrypted*** information ***segments*** in a received combined signal containing ***encrypted*** information ***segments*** and entitlement messages, wherein the demultiplexer is coupled to the decryptor for demultiplexing the combined signal following said decryption of the ***encrypted*** information ***segments*** by the decryptor; and wherein the conditional access controller is coupled to the demultiplexer for receiving the demultiplexed entitlement messages. . . . . encrypted information is provided by a plurality of information service providers in accordance with different conditional access processes respectively utilizing ***different*** ***algorithms*** for encrypting the information, comprising encryption means for ***encrypting*** information ***segments*** for transmission in accordance with different conditional access processes respectively utilizing ***different*** ***algorithms*** for encrypting the information segments; a decryptor in an information receiver for decrypting ***encrypted*** information ***segments*** received by the information receiver by processing the received ***encrypted*** information ***segments*** with a session key used for encrypting the information segments in accordance with an algorithm utilized in one of said. . . access processes; and a conditional access cont

roller in
the information receiver for selectively enabling the decryptor to
decrypt received information ***segments*** ***encrypted*** in
accordance with any of said different conditional access processes by
providing to the decryptor cryptographic information for defining the.
. . utilized in said one of said different conditional access processes for use by the decryptor to decrypt the received information
segment ***encrypted*** in accordance with said algorithm.

. . . other cryptographic information includes data for use in generating a
session key for use by the decryptor for decrypting information
segments ***encrypted*** in accordance with the algorithm
utilized in said one of said different conditional access processes; and
the conditional access controller. . .
. . . medium for use in an access control processor included in an
information receiver of a conditional access system in which
encrypted information ***segments*** provided by a plurality
of information service providers are encrypted for transmission in
accordance with different conditional access processes respectively
utilizing ***different*** ***algorithms*** for encrypting the
information segments, and including a decryptor for decrypting
encrypted information ***segments*** received by the
information receiver by processing the received ***encrypted***
information ***segments*** with a session key used for encrypting
the information segments in accordance with an algorithm utilized in one
of said. . . medium is configured so as the cause the conditional
access controller to selectively enable the decryptor to decrypt
received information ***segments*** ***encrypted*** in
accordance with any of said different conditional access proces

ses, by
providing to the decryptor cryptographic information for defini ng the.
. . utilized in said one of said different conditional access processes for use by the decryptor to decrypt the received info rmation
segment ***encrypted*** in accordance with said alg orithm.

. . . controller to detect within an information stream received b y the
information receiver cryptographic information for defining the algorithm used for ***encrypting*** information ***segmen ts***
in accordance with said one of said different conditional acces s
processes and to download the detected cryptographic informatio n from
said. . .
. . . encrypted information is provided by a plurality of informat ion
service providers in accordance with different conditional acce ss
processes respectively utilizing ***different*** ***algor ithms***
for encrypting the information, comprising the steps of: (a)
encrypting information ***segments*** for transmiss ion in
accordance with different conditional access processes respecti vely
utilizing ***different*** ***algorithms*** for encrypti ng the
information segments; (b) using a decryptor in an information r eceiver
to decrypt ***encrypted*** information ***segments*** r eceived
by the information receiver by processing the received ***enc rypted***
information ***segments*** with a session key used for encr ypting
the information segments in accordance with an algorithm utiliz ed in one
of said conditional access processes; and (c) in the informatio n
receiver, selectively enabling the decryptor to decrypt receive d
information ***segments*** ***encrypted*** in accordanc e with

any of said different conditional access processes by providing to the decryptor cryptographic information for defining the. . . utilized in said one of said different conditional access processes for use by the decryptor to decrypt the received information ***segment*** ***encrypted*** in accordance with said algorithm.

. . . of: (d) detecting within an information stream received by the information receiver cryptographic information for defining the algorithm used for ***encrypting*** information ***segments*** in accordance with said one of said different conditional access processes; and (e) downloading the detected cryptographic information from said. . .

. . . step of: (d) providing the cryptographic information from a memory in the information receiver storing cryptographic information for defining said ***different*** ***algorithms*** respectively utilized in said different conditional access processes.

. . . the service providers, and (e) selecting for decryption in accordance with a predetermined priority based upon said status determinations the ***encrypted*** information ***segment*** provided by one of said service providers.

. . . of: (f) providing the cryptographic information for defining the algorithm to the decryptor in accordance with said selection of the ***encrypted*** information ***segment*** provided by said one service provider.

. . . the cryptographic information includes data for use in generating a session key for use by the decryptor for decrypting information ***segments*** ***encrypted*** in accordance with said one

conditional access process.

```
NCL     NCLM:  705/054.000
        NCLS:    ***380/047.000***  ;   ***380/228.000***
:d pn


L19  ANSWER 1 OF 1  USPATFULL
PI      US 5796829  19980818
        WO 9608912  19960321
:end



=> d hist

     (FILE 'HOME' ENTERED AT 14:21:34 ON 29 FEB 2000)

     FILE 'USPATFULL' ENTERED AT 14:21:40 ON 29 FEB 2000
L1             0 S DIFFERENT (2A) ALGORITHM# (2A) ENCRYPTION (3A) BLOCK
#
L2             0 S DIFFERENT (2A) ALGORITHM# (2A) ENCRYPTION (3A) SEGME
NT#
L3            79 S DIFFERENT (2A) ALGORITHM# (2A) ENCRYPTION
L4            12 S L3 (P) (SEGMENT# OR BLOCK#)
L5             2 S ENCRYPTION OBJECT
L6             0 S 5577125.PN.
L7             0 S 5577125/PN
L8             0 S 5577125
L9             1 S L5 AND (DOUBLE CLICKING)
L10            0 S L9 AND OOP
L11            0 S L9 AND (OBJECT ORIENTED)
L12         3681 S OBJECT ORIENTED
L13           15 S L12 AND ENCRYPTION (2A) OBJECT
L14           84 S ENCRYPT? (2A) SEGMENT?
L15           61 S L14 AND (713/NCL OR 380/NCL)
L16           63 S ENCRYPT? (1A) SEGMENT?
L17           44 S L16 AND (713/NCL OR 380/NCL)
L18         1087 S DIFFERENT ALGORITHM#
L19            1 S L17 AND L18

=> d hist

     (FILE 'HOME' ENTERED AT 16:46:38 ON 01 MAR 2000)

     FILE 'USPATFULL' ENTERED AT 16:46:46 ON 01 MAR 2000
```

08989261

L1 72 S ONE TIME PAD
L2 1 S L1 (P) (CHANGING OR DYNAMIC)

=> d kwic

L2 ANSWER 1 OF 1 USPATFULL
SUMM Other modern encryption systems have attempted to simulate the key
generation process of a ***one*** ***time*** ***pad*** by
using pseudo-random generators which creates a long series of keys
having the statistical property of randomness. Patents on such.
keys and using them to decrypt the transmitted ciphertext. Thus the
system can change keys as often as desired, even ***changing*** the
key for every block to be encrypted. The use of pseudo-random generators
has greatly enhanced the strength of many systems, but it does not
perfectly create a ***one*** ***time*** ***pad*** .

=> d pn

L2 ANSWER 1 OF 1 USPATFULL
PI US 5003596 19910326

:1

L5 ANSWER 1 OF 3 USPATFULL
CLM What is claimed is:
. . . method according to claim 17, wherein the step of generating two or
more round keys further includes the steps of: ***dividing*** the
original ***key*** into a first key and a second key of equal
length; processing the first key using a ***hash*** function to
obtain a first set of intermediate keys; and processing the second key

using a ***hash*** function to obtain a second set of intermediate keys.

37. The system according to claim 36, wherein the key processor further comprises: a ***key*** separator for ***dividing*** the original ***key*** into a first key and a second key of equal length; a first ***hashing*** processor for processing the first key using a ***hash*** function to obtain a first set of two or more intermediate keys; and a second ***hashing*** processor for processing the second key using a ***hash*** function to obtain a second set of two or more intermediate keys.

NCL NCLM: ***380/029.000***
NCLS: ***380/037.000***
:2

L5 ANSWER 2 OF 3 USPATFULL
CLM What is claimed is:
. . . monotonic, single valued function having a value for its independent variable which is a product of an integer times a ***hashed*** value characteristic of said selected publisher; said key value capable of being read by a book validation program to enable. . . system, said key value by determining an inverse value for a customized inverse monotonic, single valued function expression using said ***key*** value, ***dividing*** said inverse value by said ***hashed*** value to obtain a quotient value and determining if said quotient value is an integer.

. . . monotonic, single valued function having a value for its independent variable which is a product of an integer times a ***hashed*** value

characteristic of said selected publisher; said key value capable of being read by a book validation means to enable. . . validating said key value by determining an inverse value for a customized inverse monotonic, single valued function expression using said ***key*** value, ***dividing*** said inverse value by said ***hashed*** value to obtain a quotient value and determining if said quotient value is an integer.

NCL NCLM: 705/051.000
NCLS: ***380/028.000*** ; ***380/277.000*** ; 704/001.000;
707/500.000; ***713/168.000***
:3

L5 ANSWER 3 OF 3 USPATFULL
DETD . . . is to use a means similar to Cipher Block Chaining (CBC) mode,
as defined for the DEA. In this case, ***key*** record is ***divided*** into blocks whose length is such that each block can be
encrypted with the asymmetric key algorithm. After each step. . .
step 522 control vector and key record are concatenated to form an
intermediate value called HA-IN. At step 523, a ***hash*** value
HASH2 is calculated on HA-IN using ***hash*** algorithm ha2.
For example, ***hash*** algorithm ha2 may be the MDC-2 algorithm of
FIG. 5 and ***HASH2*** a 128-bit MDC value. The value ***HASH2***
is for practical purposes defined to be the key authenticator record
(KAR). However, the KAR may contain additional data besides
HASH2 . At step 524, KAR is decrypted with private master key PR0
to produce dPR0(KAR). In public key cryptography, the ciphertext. . .
NCL NCLM: ***380/277.000***
NCLS: ***380/030.000*** ; ***380/280.000***